REMARKS

This amendment is responsive to the Office action mailed March 22, 2004 for the above-captioned application.

- The specification, drawings and claims have been objected to for informalities.
- Claims 1-23 and 25-30 have been rejected under 35 USC 103(a).
- Claims 1, 9, 10, 13-15, and 22 are amended.
- No claims are added.
- No claims are canceled.
- Claim 24 is indicated as not having been entered.
- Claims 1-23 and 25-30 remain pending.

Objections

The drawings have been objected to based on the figure numbers. Figs. 3 and 4 have been renumbered as per the examiner's suggestion. Formal drawings are enclosed.

The specification has been amended as per the examiner's suggestions.

The omission of claim 24 is noted. The descriptor 'not entered' has been included to indicate there was no claim 24. If an alternative descriptor is preferred, the examiner's suggestion would be welcome.

The Cited Art

Claims 1-12, 14-21, 23 and 25-30 have been rejected under 35 USC 103(a) as being unpatentable over U.S. Patent No. 6,625,734 (Marvit et al.) in view of U.S. Patent No. 6,301,660 (Benson). Claim 13 and 22 have been rejected under 35 USC 103(a) as being unpatentable over Marvit et al. in view of Benson, and further in view of Mack et al.

Marvit discloses a method for controlling access to disseminated information using

encryption and a key. To read an encrypted message a recipient obtains a key for the message from a key repository. A policy manager is employed to control which recipients are granted keys. Examples of policy criteria for determining whether a recipient is authorized access to a message include: message expiration date (col. 10, line 58), whether recipient is part of an authorized group, (col. 10, lines 43-46), whether message subject matter is to be rendered inaccessible (col. 9, lines 52-64). Marvit does not disclose any limitations on the recipient's access or dissemination of the message once decrypted. Marvit does not disclose any limitation on the number of times a recipient can decrypt a given message.

Benson discloses a computer system for protecting files against unauthorized use or copying. The examiner cites Benson at col. 10, lines 46-49 and lines 65-67 as teaching the claim 1 steps of reformatting the decrypted message into a prescribed format and deleting the source-formatted decrypted message. The examiner refers to a temporary file. However, the passages cited by the examiner relates to encryption and inserting security fields. The passages do not relate to the decryption of a message, nor to the deletion of the decrypted message. Further, the temporary file referred to by the examiner is being used to create the protected file, (see col. 11, lines 3-7), and is not a decrypted file. As to the user accessing the protected files, a viewer program is provided which uses the protected file (Col. 13, lines 56-58).

Mack discloses a method for downloading a special code from a computer to a peripheral device during the boot up routine of the peripheral device. The codes are used to allow testing of the peripheral during manufacturing test cycles and to allow diagnostic testing of an installed product. Only those portions essential for implementing the special code are enabled. As a result, interrupts may be disabled during the test, (see col. 3, lines 25-55). Mack does not disclose disabling interrupts to prevent unauthorized copying.

The Claimed Inventions Distinguished

Claims 1, 9, 13, 14 and 15 are in independent format. **Claim 1** distinguishes over the cited art based at least upon the following claim limitations:

- when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, deleting the decryption key and preventing access to the decrypted message in the source format after said reformatting by deleting the source-formatted decrypted message.

Claim 1 is directed to a communication method in which the receiver is prevented from unauthorized copying of a message in its original source format. Specifically, when the receiver is authorized to view a message, a key is received. The message then is decrypted and reformatted. The key and the decrypted message are deleted. The reformatted message is available to the receiver. By deleting the key and the decrypted message in it source format, the user's access to the message is limited to the prescribed format. Note that in a dependent claim the prescribed format is the bit-mapped display format. Thus, a copy of the source is not available to the recipient. This prevents unauthorized copying or re-use of the message.

Marvit does not disclose any limitations on the recipient's access or dissemination of the message once decrypted. Benson does not disclose preventing access to a decrypted message in its source format after a step of reformatting by deleting the source-formatted decrypted message. Accordingly, the cited art does not disclose or suggest preventing access to a decrypted message in its source format after a step of reformatting by deleting the source-formatted decrypted message.

Claims 2-8 and 10-12 depend from claim 1, and distinguish over the cited art for the same reasons as given for claim 1. Claim 10 further distinguishes over the cited art based on the following limitations:

- the source-formatted decrypted message is deleted after said reformatting without having been stored in permanent memory,
- the prescribed format is a display format, and wherein the display formatted message is not retained after being displayed.

Thus, the decrypted source format is deleted and the reformatted message is not retained once displayed. None of the cited art discloses methods in which the receiver is unable to retain a copy of the decrypted message.

Independent **claim 9** distinguishes over the cited art based at least upon the following claim limitations:

- when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, deleting the decryption key and the source-formatted decrypted message;
- in which the step of processing the request at the management module to determine whether the receiver is permitted to view the message comprises: maintaining a count of a number of times that the decryption key has been sent to the receiver, testing said at least one of the plurality of parameters accessible to the management module to determine whether the count exceeds a maximum number of times to send the decryption key to the receiver, and denying permission to decrypt the message when the count exceeds the maximum number.

Claim 9 is directed to a method in which the decrypted message's source format is deleted, and in which a receiver is denied permission to decrypt the message after the key has been sent to the receiver for a maximum number of times. Marvit does not disclose any limitations on the recipient's access or dissemination of the message once decrypted. Benson does not disclose deleting the source-formatted decrypted message. None of the cited art discloses testing to determine whether a maximum number of times to send the decryption code has been exceeded, nor of denying permission to decrypt the message when the maximum number is exceeded.

Independent **claim 13** distinguishes over the cited art based at least upon the following claim limitations:

- when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, deleting the decryption key and the source-formatted decrypted message;

- wherein during the steps of decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message, interrupts are disabled at the receiver to prevent unauthorized access to the source format.

Claim 13 is directed to a method in which the decrypted message's source format is deleted, and in which interrupts are disabled curing the decrypting, reformatting and deleting steps to prevent unauthorized access to the source-formatted decrypted message. Marvit does not disclose any limitations on the recipients access or dissemination of the message once decrypted. The cited art, and particularly Benson, do not disclose deleting the source-formatted decrypted message. The cited art, and particularly Mack, do not disclose disabling interrupts to prevent unauthorized access to a secure message.

Independent **claim 14** distinguishes over the cited art based at least upon the following claim limitations:

- when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message without first storing the decryption key and source-formatted decrypted message in a permanent memory.

Claim 14 is directed to a method in which the decrypted message's source format is deleted without being stored in permanent memory to prevent unauthorized access to the source-formatted decrypted message. The cited art does not disclose or suggest such deletion.

Independent **claim 15** distinguishes over the cited art based at least upon the following claim limitations:

- processing means at the receiver for decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message without

first storing the decryption key and source-formatted decrypted message in a permanent memory.

Claim 15 is directed to a system in which the decrypted message's source format is deleted without being stored in permanent memory to prevent unauthorized access to the source-formatted decrypted message. The cited art does not disclose or suggest such deletion.

Claims 16-30 depend ultimately from claim 15 and distinguish over the cited art for the same reasons as given for claim 15. **Claim 16** further distinguishes over the cited art based upon the following claim limitations:

- wherein the plurality of parameters comprises: a maximum number of times that the secure message is permitted to be decrypted.

Claim 22 further distinguishes over the cited art based upon the following claim limitations:

- means for disabling interrupts at the receiver to prevent unauthorized access to the source-formatted decrypted message, while the processing means decrypts the message into the source format, reformats the decrypted message into the prescribed format, and deletes the decryption key and the source-formatted decrypted message.

Conclusion

In view of the above remarks regarding the cited art, it is respectfully submitted that the claims contain key limitations that are not present in the cited art and not obvious from the cited art. These particular limitations, are not disclosed in or suggested by cited references. These limitations are significant advances over the prior art and resulted in a novel method and apparatus for securing communications.

In view of the above amendments and remarks, it is respectfully submitted that the claims are now in condition for allowance. The Examiner's action to that end is respectfully requested. Reconsideration of the claims and withdrawal of the rejections is respectfully requested.

Reinstatement of the dependent claims drawn to non-elected species is requested upon allowance of the generic claims from which they depend.

If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the application, the Examiner is invited to call the undersigned attorney at the telephone number given below.

Respectfully submitted,

Dated: 5-25-04 By: _____

Steven P. Koda
Reg. No. 32,252
Tel.: 360-859-4013

Koda Law Office
8070 E. Mill Plain Blvd, No. 141
Vancouver, WA 98664-2002